Appendix A

SPECIAL CONSIDERATIONS FOR SAFEGUARDING PERSONAL INFORMATION IN ADP SYSTEMS

(See subsection D.2. of Chapter 1)

A. GENERAL

1. The Automated Data Processing (ADP) environment subjects personal information to special hazards as to unauthorized compromise alteration, dissemination, and use. Therefore, special considerations must be given to safeguarding personal information in ADP systems.

2. Personal information must also be protected while it is being processed or accessed in computer environments outside the data processing installation (such as, remote job entry stations, terminal stations, ❑inicomputers, micro-processors, and similar activities).

3. ADP facilities authorized to process classified material have adequate procedures and security for the purposes of this Regulation. However, all, unclassified information subject to this Regulation must be processed following the procedures used to process and access information designated “For Official Use Only” (see DoD 5400.7-R, reference (f)).

B. RISK MANAGEMENT AND SAFEGUARDING STANDARDS

1. Establish administrative, technical, and physical safeguards that are adequate to protect the information against unauthorized disclosure, access, or misuse (see Transmittal Memorandum No. 1 to OMB Circular A-71, reference (s)).

2. Technical and physical safeguards alone will not protect against unintentional compromise due to errors, omissions, or poor procedures. Proper administrative controls generally provide cheaper and surer safeguards.

3. Tailor safeguards to the type of system, the nature of the information involved, and the specific threat to be countered.

C. MINIMUM ADMINISTRATIVE SAFEGUARD

The minimum safeguarding standards as set forth in subsection D.2. of Chapter 1 apply to all personal data within any ADP system. In addition:

1. Consider the following when establishing ADP safeguards:

   a. The sensitivity of the data being processed, stored and accessed;

   b. The installation environment;

   c. The risk of exposure;

   d. The cost of the safeguard under consideration.

2. Label or designate output and storage media products (intermediate and final) containing personal information that do not contain classified material in such a manner as to alert those using or handling the information of the need for special protection. Designating products “For Official Use Only” in accordance with DoD 5400.7-R (reference (f)) satisfies this requirement.

3. Mark and protect all computer products containing classified data in accordance with DoD 5200.1-R (reference (a)) and DoD 5200.28-M (reference (t)).

4. Mark and protect all computer products containing “For Official Use Only” material in accordance with reference (f).

5. Ensure that safeguards for protected information stored at secondary sites are appropriate.

6. If there is a computer failure, restore all protected information being processed at the time of the failure using proper recovery procedures to ensure data integrity.

7. Train all ADP personnel involved in processing information subject to this Regulation in proper safeguarding procedures.

D. PHYSICAL SAFEGUARDS

1. For all unclassified facilities, areas, and devices that process information subject to this Regulation, establish physical safeguards that protect the information against reasonably identifiable threats that could result in unauthorized access or alteration.

2. Develop access procedures for unclassified computer rooms, tape libraries, micrographic facilities, decollating shops, product distribution areas, or other direct support areas that process or contain personal information subject to this Regulation that control adequately access to these areas.

3. Safeguard on-line devices directly coupled to ADP systems that contain or process information from systems of records to prevent unauthorized disclosure use or alteration.

4. Dispose of paper records following appropriate record destruction procedures.

E. TECHNICAL SAFEGUARDS

1. The use of encryption devices solely for the purpose of protecting unclassified personal information transmitted over communication circuits or during processing in computer systems is normally discouraged. However, when a comprehensive risk assessment indicates that encryption is cost-effective it may be used.

2. Remove personal data stored on magnetic storage media by methods that preclude reconstruction of the data.

3. Ensure that personal information is not inadvertently disclosed as residue when transferring magnetic media between activities.

4. When it is necessary to provide dial-up remote access for the processing of personal information, control access by computer-verified passwords. Change passwords periodically or whenever compromise is known or suspected.

5. Normally the passwords shall give access only to those data elements (fields) required and not grant access to the entire data base.

6. Do not rely totally on proprietary software products to protect personnel data during processing or storage.

F. SPECIAL PROCEDURES

1. System Managers shall:

a. Notify the ADP manager whenever personal information subject to this Regulation is to be processed by an ADP facility.

b. Prepare and submit for publication all system notices and amendments and alterations thereto (see subsection A.6. of Chapter 6).

c. Identify to the ADP manager those activities and individuals authorized access to the information and notify the manager of any changes to the access authorizations.

2. ADP personnel shall:

a. Permit only authorized individuals access to the information.

b. Adhere to the established information protection procedures and rules of conduct.

c. Notify the system manager and ADP manager whenever unauthorized personnel seek access to the information.

3. ADP installation managers shall:

a. Maintain an inventory of all computer program applications used to process information subject to this Regulation to include the identity of the systems of records involved.

b. Verify that requests for new programs or changes to existing programs have been published as required (see subsections D.1. and 2. of Chapter 6).

c. Notify the system manager whenever changes to computer installations, communications networks, or any other changes in the ADP environment occur that require an altered system report be submitted (see subsection D.2. of Chapter 6).

G. RECORD DISPOSAL

1. Dispose of records subject to this Regulation so as to prevent compromise (see subsection D.3. of Chapter 1). Magnetic tapes or other magnetic medium, may be cleared by degaussing, overwriting, or erasing. Unclassified carbon ribbons are considered destroyed when placed in a trash receptacle.

2. Do not use respliced waste computer products containing personal data.

H. RISK ASSESSMENT FOR ADP INSTALLATIONS THAT PROCESS PERSONAL DATA

1. A separate risk assessment is not required for ADP installations that process classified material. A simple certification by the appropriate ADP official that the facility is cleared to process a given level of classified material (such as, Top Secret, Secret, or Confidential) and that the procedures followed in processing "For Official Use Only" material are to be followed in processing personal data subject to this Regulation is sufficient to meet the risk assessment requirement.

2. Prepare a formal risk assessment for each ADP installation (to include those activities with terminals and devices having access to ADP facilities) that processes personal information subject to this Regulation and that do not process classified material.

3. Address the following in the risk assessment:

a. Identify the specific systems of records supported and determine their impact on the mission of the user.

b. Identify the threats (internal, external, and natural) to the data.

c. Determine the physical and operational (to include software) vulnerabilities.

d. Evaluate the relationships between vulnerabilities and threats.

e. Assess the impact of unauthorized disclosure or modification of the personal information.

f. Identify possible safeguards and their relationships to the threats to be countered.

g. Analyze the economic feasibility of adopting the identified safeguards.

h. Determine the safeguard to be used and develop implementation plans.

i. Discuss contingency plans including operational exercise plans.

j. Determine if procedures proposed are consistent with those identified in the system notices for system of records concerned.

k. Include a vulnerability assessment.

3. The risk assessment shall be reviewed by the appropriate Component officials.

4. Conduct a risk assessment at least every 5 years or when there is a change to the installation, its hardware, software, or administrative procedures that increase or decrease the likelihood of compromise or present new threats to the information.

5. Protect the risk assessment as it is a sensitive document.

6. Retain a copy of the risk assessment at the installation and make it available to appropriate inspectors and authorized personnel.

7. Include a summary of the current risk assessment with any report of new or altered system submitted in accordance with subsection D.3. of Chapter 6 for any system from which information will be processed.

8. Complete a formal risk assessment at the beginning of the design phase for each new unclassified ADP installation and before beginning the processing of personal data on a regular basis in existing ADP facility that do not process classified data.